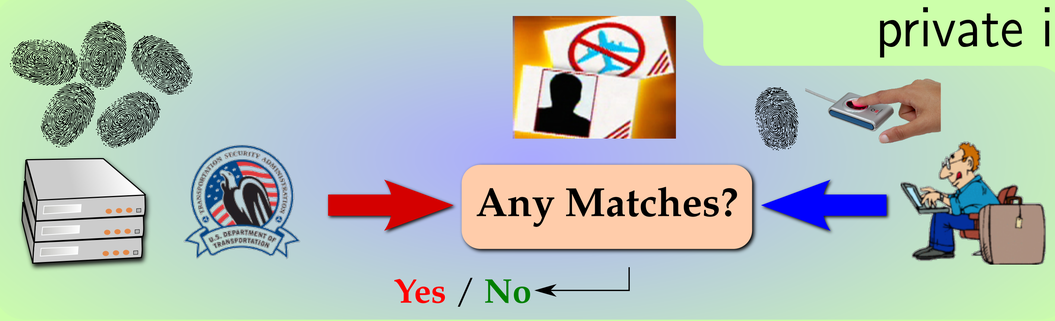
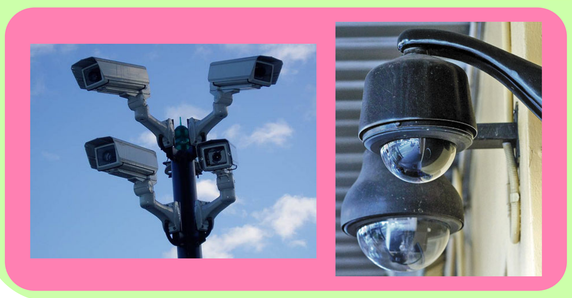
Efficient Privacy-Preserving Biometric Identification†

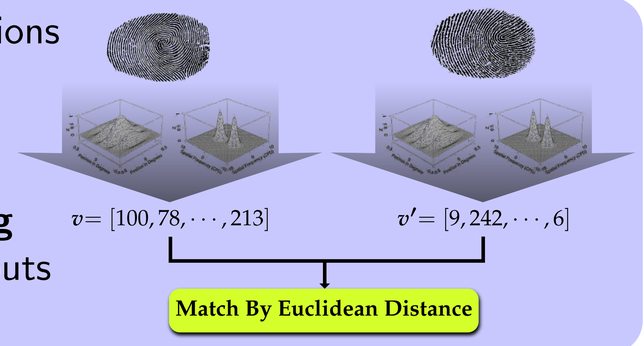
Yan Huang Dept. of Computer Science, University of Virginia
http://www.mightbeevil.org/secure-biometrics/

Motivation: Prove/disprove identity without losing private information





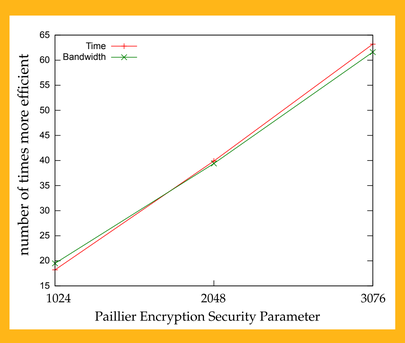
Many existing non-private solutions consist of two steps: a **feature extraction** step, that involves sophisticated image processing; and a **feature vector matching** step, the only step requiring inputs from both parties.



$$[\![d_i]\!] = \left[\!\!\left[\underbrace{\sum_{j=1}^{N} v_{i,j}^2}_{S_{i,1}} + \underbrace{\sum_{j=1}^{N} (-2 v_{i,j} v'_j)}_{S_{i,2}} + \underbrace{\sum_{j=1}^{N} v'^2_j}_{S_3} \right]\!\!\right] = [\![S_{i,1}]\!] \cdot [\![S_{i,2}]\!] \cdot [\![S_3]\!] \qquad [\![S_{i,2}]\!] = \left[\!\!\left[\sum_{j=1}^{N} (-2 v_{i,j} v'_j) \right]\!\!\right] = \prod_{j=1}^{N} [\![-2 v_{i,j}]\!]^{v'_j}$$

$$\left.\begin{matrix} [\![a]\!]_{\mathsf{pk}} \\ [\![b]\!]_{\mathsf{pk}} \end{matrix}\right\} \Rightarrow [\![a+b \mod p]\!]_{\mathsf{pk}} = [\![a]\!]_{\mathsf{pk}} \cdot [\![b]\!]_{\mathsf{pk}} \qquad \left.\begin{matrix} [\![a]\!]_{\mathsf{pk}} \\ c \end{matrix}\right\} \Rightarrow [\![c \cdot a \mod p]\!]_{\mathsf{pk}} = [\![a]\!]_{\mathsf{pk}}^{c}$$

$$\left.\begin{matrix} a_1,\ a_2,\ a_3\ _{\mathsf{pk}} \\ b_1,\ b_2,\ b_3\ _{\mathsf{pk}} \end{matrix}\right\} \Rightarrow a_1+b_1,\ a_2+b_2,\ a_3+b_3\ _{\mathsf{pk}}$$



	$51, 28, 72$	$51, 28, 72$ pk
+	$39, 92, 22$	• $39, 92, 22$ pk
	$91, 20, 94$	$91, 20, 94$ pk

	$051, 028, 072$	$051, 028, 072$ pk
+	$039, 092, 022$	• $039, 092, 022$ pk
	$090, 120, 094$	$090, 120, 094$ pk

Packed computation makes it much more efficient.

$V = \{v_1, v_2, \cdots, v_M\}$ $\qquad$ $v' = \{v'_1, v'_2, \cdots, v'_N\}$

Euclidean Distance — **Homomorphic Encryption**

$d = \{d_1, d_2, \cdots, d_M\}$

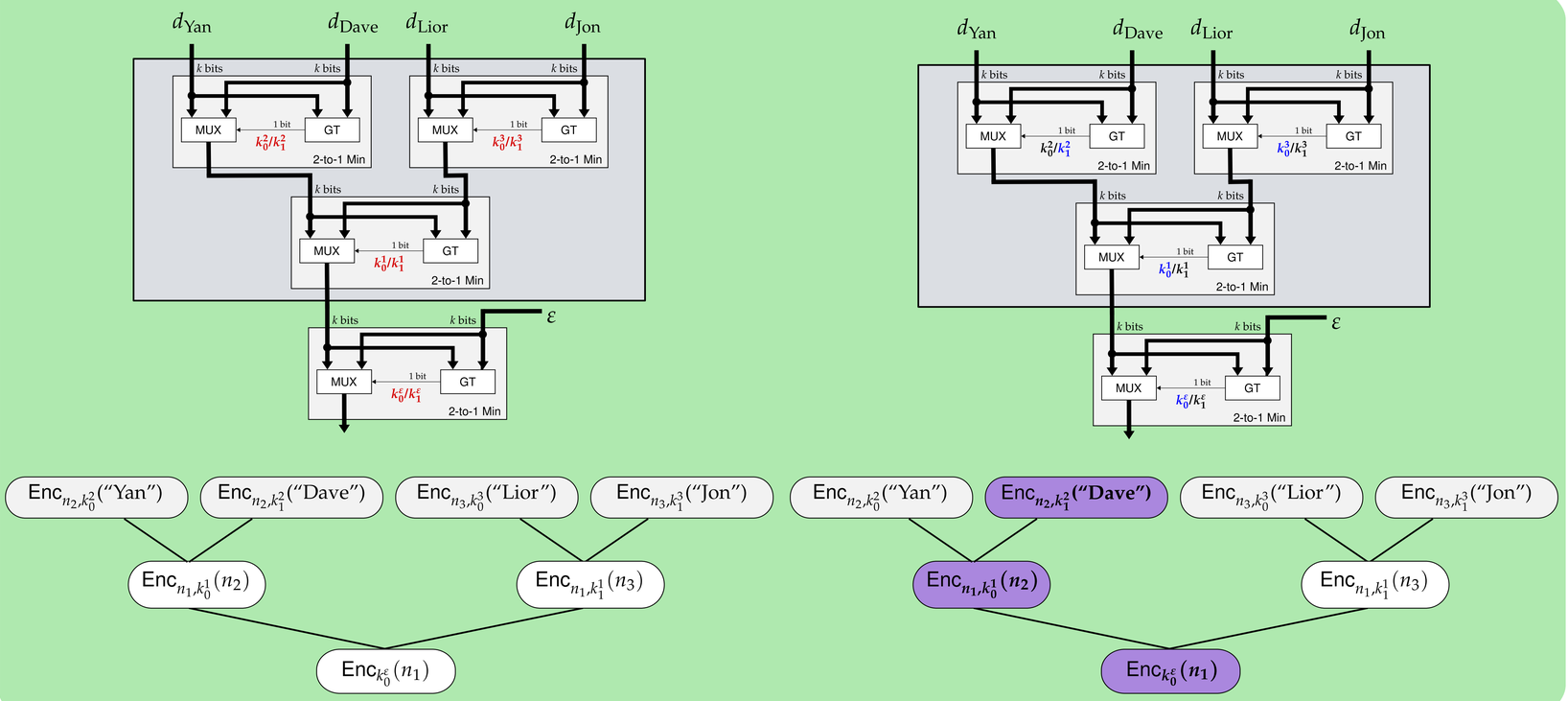
$d' = \{d'_1, d'_2, \cdots, d'_M\}$ $\qquad$ $r = \{r_1, r_2, \cdots, r_M\}$

Finding Minimum — **Garbled Circuits**

$$d^* = \min_{1 \le i \le M} (d_i)$$

Retrieve Identity

Backtracking Protocol

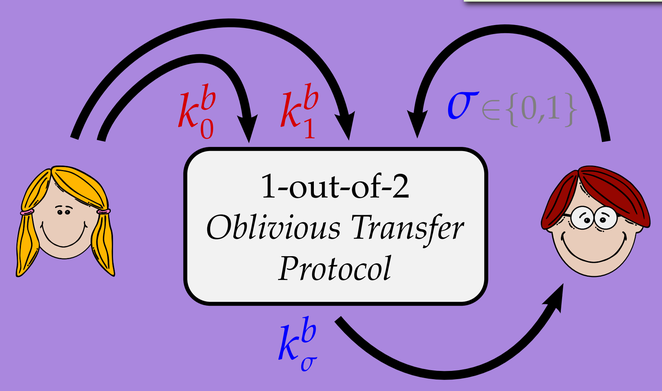


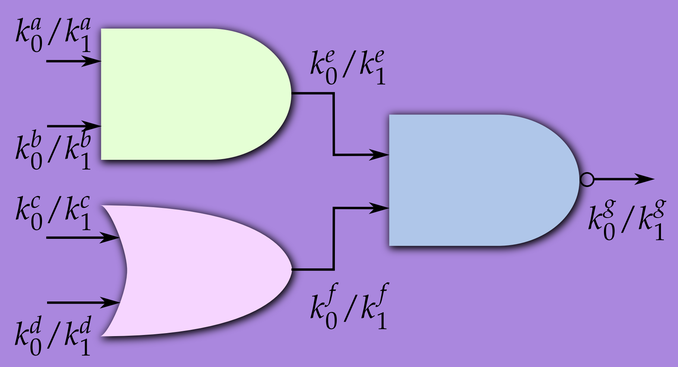
0 or 1	0 or 1	a	b	z	0 or 1
		0	0	0	
		0	1	0	
		1	0	0	
		1	1	1	

k_0^a or k_1^a	k_0^b or k_1^b	a	b	z	k_0^z or k_1^z
		k_0^a	k_0^b	k_0^z	
		k_0^a	k_1^b	k_0^z	
		k_1^a	k_0^b	k_0^z	
		k_1^a	k_1^b	k_1^z	

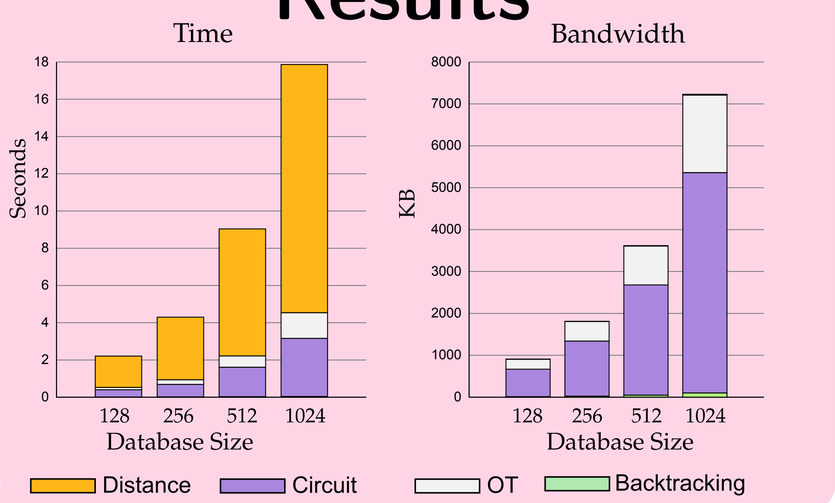
k_0^a, k_1^a	k_0^b, k_1^b		k_0^z, k_1^z
		$\text{Enc}_{k_0^a,k_0^b}(k_0^z)$	
		$\text{Enc}_{k_0^a,k_1^b}(k_0^z)$	
		$\text{Enc}_{k_1^a,k_0^b}(k_0^z)$	
		$\text{Enc}_{k_1^a,k_1^b}(k_1^z)$	

k_0^a	k_1^b		k_0^z
		$\text{Enc}_{k_0^a,k_0^b}(k_0^z)$	
		$\text{Enc}_{k_0^a,k_1^b}(k_0^z)$	
		$\text{Enc}_{k_1^a,k_0^b}(k_0^z)$	
		$\text{Enc}_{k_1^a,k_1^b}(k_1^z)$	





Results



- We compute the global minimum, which improves identification accuracy.
- Still 4.6× faster and 58% less bandwidth than best previous work.
- Privacy-preserving biometric identification can be sufficiently fast for on-line uses.

† Work done in collaboration with David Evans (advisor, UVA), Lior Malka (UMD) and Jonathan Katz (UMD).

Yan Huang, Lior Malka, David Evans, and Jonathan Katz. Efficient Privacy-Preserving Biometric Identification. In *Network and Distributed System Security Symposium*, 2011.